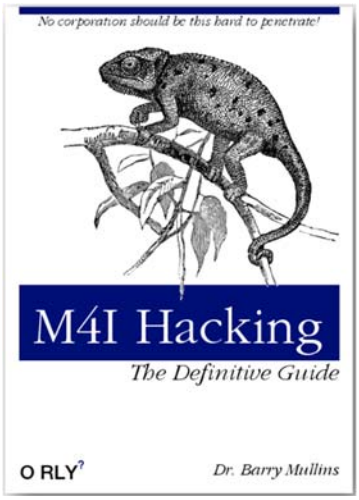
CSCE 629
Final Project
Winter 2019



Assigned: **12 Feb**
Report due: **7 Mar, 1700** **Late submissions will not be accepted**

Always remember, this final project is an assessment tool equivalent to a final exam.

- **You will work with your partner and submit one solution.**
- **You must work only with your partner.**
- **You may not receive help from anyone else.**
- **You may not use any material from students who took the course before you. This includes materials from your participation in AFIT's ACE program.**
- **You may not give or receive help in any form to other teams.**
- **Keep your voice low as you talk with your partner.**
- **Do not leave information on your computer monitor while away from your desk.**
- **You may not impede another team's efforts to complete the exercise. In other words, never DoS anything including sending de-authentication frames continuously. If needed, use de-authentication judiciously.**
- **Read these instructions completely before starting the project.**

Final project objectives:

- Tie together (synthesize) everything you have learned during the quarter.
- Understand how various techniques and tools can be used to exploit a company to harvest information and gain unauthorized access.
- Document your attack methodology and results in detail.

Final project goals:

There are several flags, files, and information on and around computers within the CDN lab as well as information on other computers. Your assignment is to find all flags and use the information/clues to decipher the phrase that pays.

Your score is based on the following. Maximum points available is **333**.

- **114** pts: Usernames and passwords correctly reported (accounts are not equally weighted).
- **58** pts: Flags correctly reported (flags are not equally weighted).
- **70** pts: Files / information (includes supplemental questions) you find that support your penetration efforts. In other words, a file (not a flag) may help you decipher a password (files are not equally weighted).
- **10** pts Following the instructions in the Course Closeout section.
- **10** pts Submitting general observations.
- **71** pts Final report.
- Your score is based on how well you document the **process** you use to find and retrieve the items of interest. For example, a password may be worth 3 points. If you simply list the password, you will receive 1 point; if you also list the detailed process, including screenshots, you used to learn the password, all three points will be awarded.

You may use lifelines to seek assistance during the exercise. All lifeline requests must be directed to the instructor; "phone a friend" and "ask a neighbor" are not allowed. Lifelines may not be free; each lifeline may cost you up to 2 points (not 2%). If in doubt, just ask, and the instructor will tell you if information is free. If you have been working on an issue for more than two hours, see me; there is the distinct possibility the target is not functioning correctly.

Send all Capture the Flag (final project) questions and requests to mullins@mail.m4i.local.

Rules of engagement (Violating these rules can result in substantial penalties)

Congratulations! You won the contract to perform a penetration test on Mullins Movies, Music and Machines Inc. (M4I) as shown in Figure 1. You are granted permission to attack the M4I network. The following information is provided in the contract provided by the chief information officer (CIO):

- During this assignment, *attack* is defined as an attempt to compromise a system by exploiting a running process (e.g., buffer overflow).
- There is a listing of IP addresses on the network; you must find these addresses and only attack IPs assigned to your team. You may NEVER attack any other address as this may bring down critical production systems.
- Due to the sensitive nature of employee passwords, M4I strictly forbids the use of any online cracking capability. For example, you may not submit known password hashes to online lookup tables (also known as reverse lookup tables) or distributed search engines. The hashes may not leave the CDN network.
- **Many** passwords are not crackable or guessed. Therefore, if a password is not cracked within one hour (depending on your system configuration), you can assume it must be learned via other means such as information found in flags/files.

Figure 1. M4I Headquarters

Always remember, you are performing a penetration test on a company's network. You do not want to open new attack vectors during your test, which could be used by external hackers to cause serious harm to the company. If this occurs, you will be held accountable.

To this end, you may NOT

- attack or modify Dr. Mullins or his computer.
- change permissions on existing files or take ownership of existing files or elevate privileges on existing users.
- attack or modify any network infrastructure (routers and switches).
- delete or modify existing files (including flags and any file permissions) or accounts (passwords) on the target systems unless explicitly directed to do so.
- add user accounts or start services on the target (e.g., start an SSH server so you can log into the machine).
- add additional flags or files with the word "flag" in them.
- disable or turn off firewall, anti-virus, or any other protection mechanisms on the target machines.
- attack other students.
- DoS any system. Be careful if you use arpspoof; you may inadvertently DoS the entire lab. It has happened.
- attempt to physically attack/access target computers.
- update/change the registries on target machines. Please do not play with the registry on the targets.
- use Rootkits. They are not necessary.
- use the AFIT CIS network to attack

Other items of interest:

- All targets have private IP addresses. Do not scan or attempt to attack any machine outside these address spaces.
- Keep your Outlook client open so you can receive my emails quickly. I do email hints and pointers to individual teams!
- You may access the Internet to gather information to complete this exercise. However, you may not attack any machine outside the CDN lab.
- You may add programs and files to the targets; delete these files once done.
- Remember to delete john.pot.
- If you feel one of your targets is not responding correctly, you may ask the instructor to check the operational status of the target.
- Flag filenames begin with flag1, flag2, … There are two flags per division. The flags may be located in any directory and may require manipulation to extract the flag information.
- Any social engineering must be convincing or the target may not bite.
- The instructor will delete any files or accounts that look suspicious.
- You are not required to crack passwords belonging to system accounts including, but not limited to, any account containing the following words: "mullins", "Install", "Iusr", "Iwam", "monitor", "support", "help", or "Guest". There is a good chance you will not be able to crack them anyway. ☺
- As soon as you find all flags, passwords for all accounts and can successfully recite the Phrase that Pays, send me an email. Your team will be "recognized" and remembered as the uber-team for this year.

- The penetration testing contract also stipulates that the CIO must have visibility into your progress. To this end, you are required to use the _teamstatus excel spreadsheet provided in your team folder. Do not rename or move the file, and do not modify the format including inserting/deleting rows/columns. Update this spreadsheet each time you find information. Use a lower case x to denote you found a flag or learned the information requested. When you discover and confirm a user's password, list the username next to the appropriate machine as shown with example names. Do **not** post passwords on this status page. I monitor this file to ensure [redacted] you are making adequate progress and provide hints, so you must update it as soon as you find information. Do not hold on to several items and enter them after several days.
- Keep your daily hours updated. Recording the hours at the end of each day works best.

	1-Alamri-Hayden-Mireles	Hours	Alamri	Hayden	Mireles
Flags/Questions		12-Feb-19	3	2	3
1	x	13-Feb-19	4	1	0.5
2		14-Feb-19	0	0	0
3		15-Feb-19	0	0	0
4		16-Feb-19	0	0	0
5		17-Feb-19	0	0	0
6		18-Feb-19	0	0	0
7		19-Feb-19	0	0	0
8		20-Feb-19	0	0	0
9		21-Feb-19	0	0	0
10		22-Feb-19	0	0	0
11		23-Feb-19	0	0	0
12		24-Feb-19	0	0	0
13		25-Feb-19	0	0	0
14		26-Feb-19	0	0	0
15		27-Feb-19	0	0	0
16		28-Feb-19	0	0	0
17		1-Mar-19	0	0	0
18	x	2-Mar-19	0	0	0
19		3-Mar-19	0	0	0
20		4-Mar-19	0	0	0
21		5-Mar-19	0	0	0
22		6-Mar-19	0	0	0
Restaurants		7-Mar-19	0	0	0
Heartbeat pwd	x	Total	7	3	3.5
Key	WEP				
Key					
Key					
Marketing	Mullins				
Machine	Blackhat				

You are not required to

- recommend remediation actions for any vulnerabilities found
- discuss covering your tracks
- discuss maintaining access

Final report

The key word for the report is CONCISE!

- Your target audience is the M4I IT staff. Your report should contain enough details such that the IT staff (not the brightest bunch) can replicate your results. **The IT staff prefers bullet format.**
- As you prepare your final report, remember the IT staff needs to understand exactly how you were able to gain access to all boxes as well as find and display the flags/files/information. A useful technique is to take screenshots and include the command in the image. This also applies to nmap scans—include the nmap command in the image. Ensure the path is included in all files/flags mentioned in the report; in other words, I need to know where you found evidence.
- You may not show an example usage of a command or tool early in the report and state that the same (or similar) command is used for all targets. Provide the commands as used on each target.
- **The report must contain detailed instructions including tools and/or exact commands used.**
  - **If you used a tool, be sure to include how you configured the tool.**
  - **You are not required to provide instructions on how to install a tool.**
  - **If you use a command line, be sure to include the exact command entered.**
  - **If you leverage another team's efforts such as using a device that was left on, you still must document how the IT staff can turn on the device. In other words, you cannot monitor another team's actions and reap the benefits; you must document how to cause the effect.**
- The IT staff requires a screenshot of each flag being displayed on the terminal as proof the M4I systems are vulnerable. Provide these screenshots in the section discussing the division where you found the flag.
- The IT staff also needs a screenshot of each cracked password in John or Cain for each division. In other words, be sure to take a screenshot when a tool cracks/verifies a password. **This is the only acceptable confirmation of a valid password.** Using the password to log into a service is not acceptable as the password is not displayed during this process.
- If you make any additions to your host's networks, you must provide explanation along with diagrams.
- You may want to use photographs where a screenshot is not feasible; this proves you actually found the information.
- The IT staff is minimally manned and cannot afford to read about unproductive attempts to penetrate their systems. They are only interested in successful attacks; unsuccessful attacks mean the target systems are not vulnerable and therefore require no additional attention. Therefore, they do not want a listing/discussion of unproductive paths or techniques; report just what worked.
- It is your responsibility to keep the report succinct yet covering all vital information. You should NOT include 100 pages of Nessus scan results; distill the information for the IT staff.

The report must include the following in the order shown. **The IT staff prefers bullet format!**

- Cover page (make it interesting with a creative team name).
- Network map of M4I.
  - You may not simply provide the nmap topology output as your map; create the map in a tool like Visio, PowerPoint, etc. showing all devices (servers, switches, routers, etc.) and IP addresses (ports are not required) for all interfaces.
  - Do not use a jpg or gif background/watermark.
  - Include machines you interacted with; do not include machines being attacked by the other teams.
  - Include any M4I machines dedicated to hosting services (e.g., web servers, FTP servers…).
  - Include all of your attack machines in the map.
- A section dedicated to each division you attacked. Start each section on a new page. The compromised computers must be discussed in the order listed in the _teamstatus spreadsheet. You must provide screenshots to convince the IT staff you accomplished all tasks.
  - Each section should give all details of the attack. Your description should include the following **in the order shown** as a minimum:
    - How did you find the target?
    - How did you gain access to the target?
      - Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.

        - If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
        - What tool(s) or commands did you use to exploit the system?
    - How did you learn usernames?
    - How did you learn passwords?
    - How did you find and download flags?
    - How did you find and download any other files you may have harvested from the target?

- Table showing all account usernames and passwords. If you cannot find a user's password, include the username but leave the password entry blank. Include an empty row if you could not find the username or password. Table columns should be as follows and illustrated:
    - Number each row
    - Division Name
    - Username (remember some usernames are case sensitive)
    - Password
    - Account type (user or admin/root)

#	Division	Username	Account Type	Password
1	Marketing	Superman	Admin	I-fly
2		WonderWoman	User	Invisible
3		Spiderman	User	web
4		TomHanks	User	Big
5	Machine	Roger	User	Rabbit
6		Terminator		
7		SnowWhite		
8				
9	Music			

- Supplemental questions: An appendix containing the answers to the following questions. As always, include the question in the appendix and provide supporting evidence (i.e., screenshots and detailed explanations) detailing how you found the information.
    1. List the restaurants Dr. Evil visits frequently.
    2. What is the password learned from the Heartbeat Server?
- An appendix containing the source code for any programs or scripts you wrote and used during the exercise.
- An appendix answering the **General Observations**:
    - You are required to keep a log of time spent on this assignment and include the log in this appendix.
    - How long (in wall clock hours; not man hours) did it take to complete the project excluding the report?
    - How long (in wall clock hours; not man hours) did it take to prepare the report?
    - Was it an appropriate length final assignment considering the time allotted?
    - What corrections and or improvements do you suggest for this project? Please be specific, and if you add new material, give the exact wording/instructions you would give future students in the new project handout. Feel free to cross out and edit text to make minor corrections/suggestions.

The report must adhere to the following formatting guidelines:

- Add page numbers to each page in the lower right corner except the cover page.
- Use Times New Roman 11 point font for text. You may use smaller font for tables so they fit on one page.
- Use portrait orientation; do not use landscape unless your figure (e.g., network map) is best displayed in landscape.
- **Print in color using single-sided pages.**
- Ensure figures, tables and screenshots are legible to the CIO, who uses reading glasses and does not like using a magnifying glass to read tiny print.
- Do not staple or bind the pages together in any way; I will provide a binder clip.

Advice

- Keep good notes on how you accessed each machine.
- Maintain a network map as you progress through the exercise. This helps visualize potential attack vectors.
- You will most likely have to return to some machines even when you think you are done with them. This may be due to forgetting to take screenshots or learning more information that could be helpful to machines you compromised earlier.
- You may not find all the credentials for a box immediately; you may have to proceed with your pen test to find additional information required to determine a password.

Course Closeout

Your final assignment is to clean up your team folder on the CDN fileserver. Verify you have a folder called Mullins in your team folder and placed the following files there using the naming convention shown:

- Reports for labs. Be sure to include both lab 1 reports
- CTF report in Word (if available) **and** PDF format
- Project reports

Do not create subfolders for the labs. Your directory should resemble Figure 2.

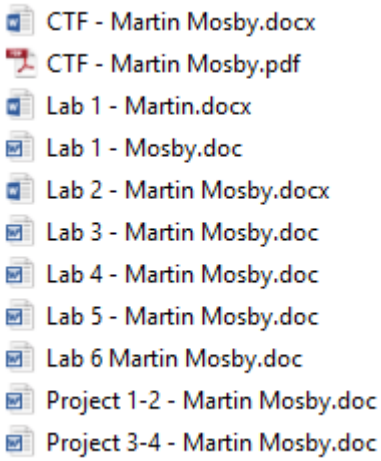


Figure 2. Example of Mullins folder contents